CCDCOE

NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

1 November 2019

DISCLAIMER

This presentation is a product of the CCDCOE but does ***not*** reflect the policy or the opinion of NATO or any of the CCDCOE Member Nations.

The CCDCOE is a **cyber defence think tank, training and exercise facility.**

As a community of 25 nations, the CCDCOE holds expertise in the areas of technology, strategy, operations and law and provides a 360-degree look at cyber defence.

The CCDCOE is ***not*** part of the NATO command structure.

CCDCOE

5G

Should we worry about Huawei?

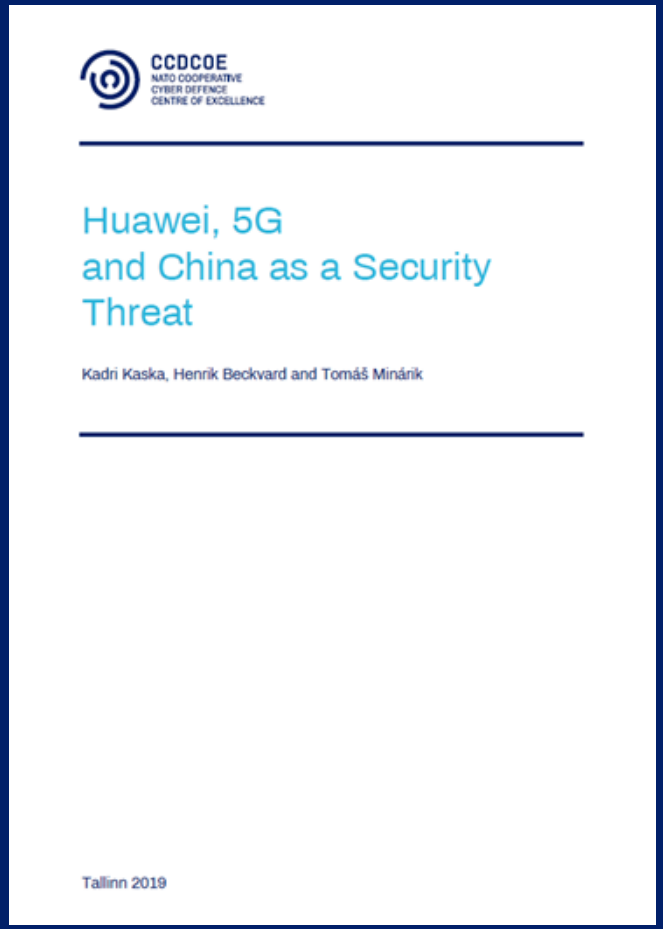
CCDCOE

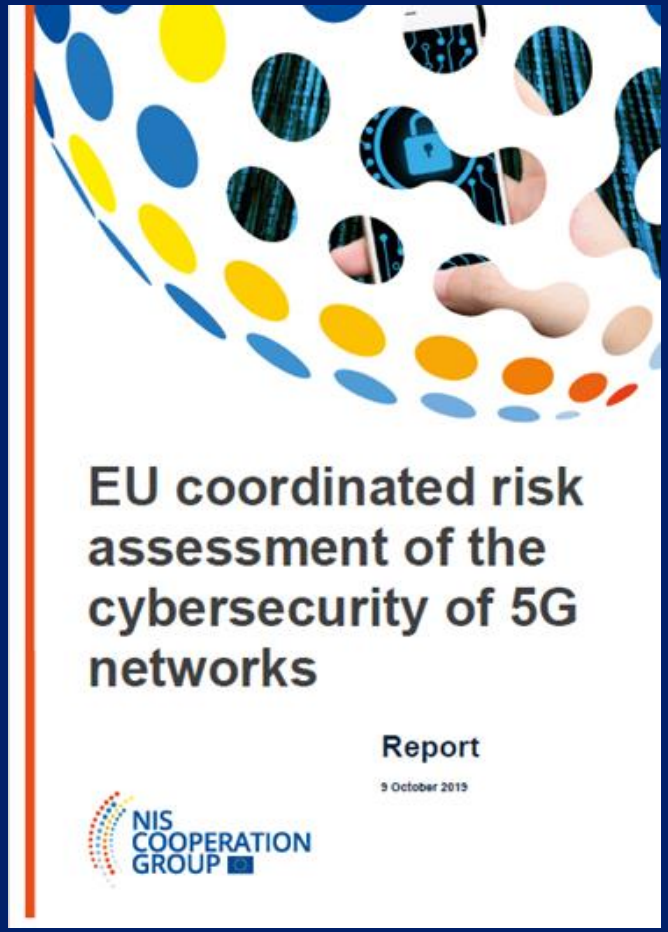
What is 5G?

As the new *'digital nervous system'* of modern societies it is awesome, *but*…

- **It comes with a lot of security concerns also**
- **IoT will bring new cyber attack vectors**
- **Once installed by a provider, 5G is not easily reversed or replaced**

CCDCOE


CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE
Huawei, 5G
and China as a Security
Threat
Kadri Kaska, Henrik Beckvard and Tomáš Minárik
Tallinn 2019


EU coordinated risk
assessment of the
cybersecurity of 5G
networks
Report
9 October 2019
NIS
COOPERATION
GROUP

CCDCOE

Why Huawei?

It is necessary to look at Huawei & 5G in a wider context and not just as a choice of technology

There are no known exploitable vulnerabilities to date *but*…

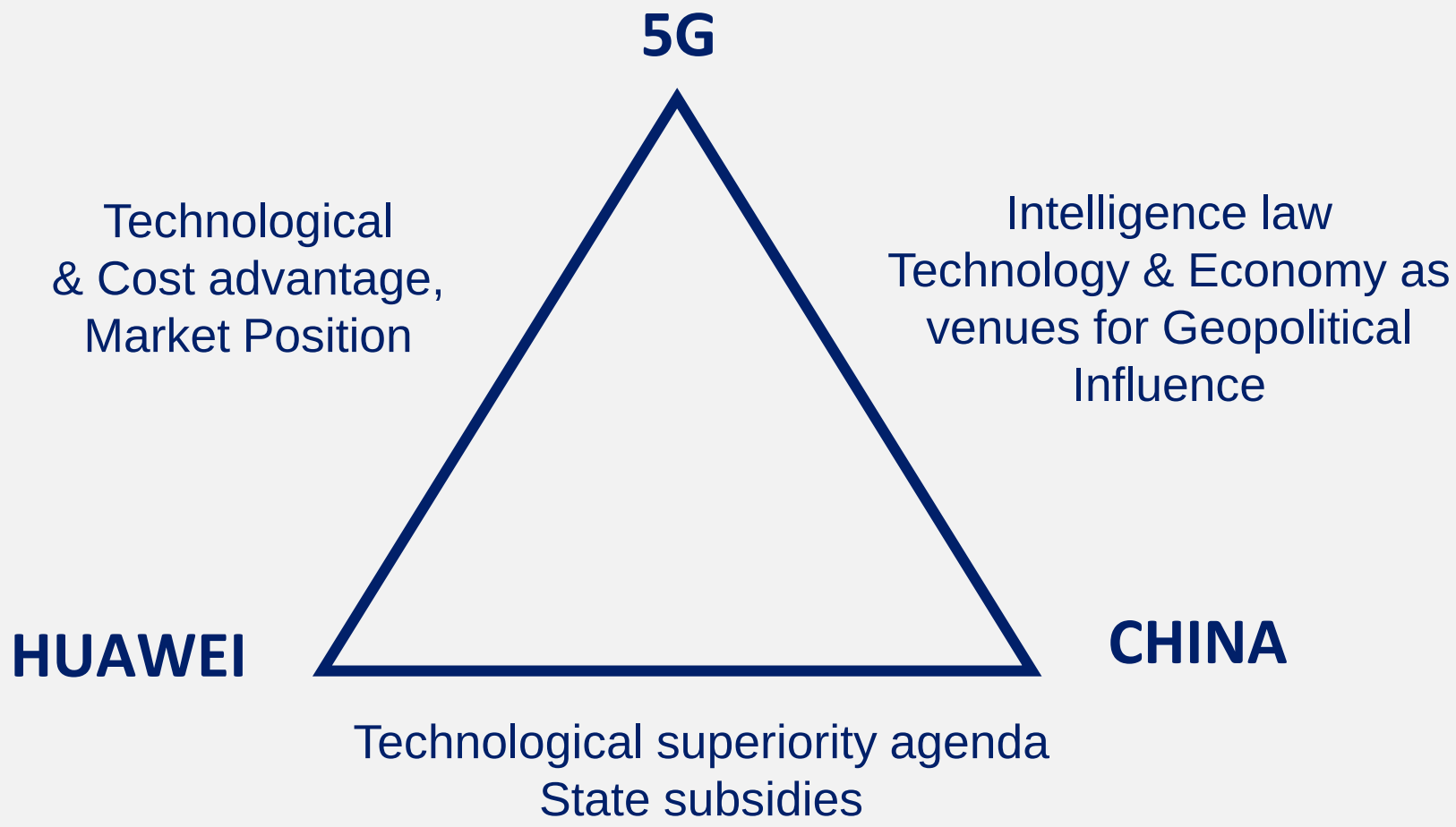
- a track record of industrial espionage,
- violating sanctions regime,
- staff alleged to have engaged in espionage for the Chinese government

CCDCOE

Who is leading the race to develop 5G?

1. Huawei (CHN)
2. Ericsson (SWE)
3. Hisilicon (CHN)
4. Nokia (FIN)
5. QUALCOMM (USA)
6. Samsung Electronics (ROK)
7. ZTE (CHN)

Why Huawei?



CCDCOE

Security environment:
China’s strategic reinforcement of its interests

China has a national technological superiority agenda:

- The State is subsidising technology sector and R&D,
- Market barriers for foreign providers
- Practice of espionage and influence operations:
- Notorious reputation for state-sponsored industrial espionage involving private actors (overwhelming evidence over the years)
- Legal and political environment: legal obligation for companies to cooperate with intelligence agencies,
- Political environment conducive to such cooperation, lack of constraints and accountability

CCDCOE

China’s Belt and Road Initiative (BRI)

Reinforcement of China’s strategic interests

CCDCOE

International law constraints

The influence exerted over Chinese companies by their government and military

- The Chinese National Intelligence Law of 2016 requires all companies to support, provide assistance to, and cooperate in national intelligence work

Espionage as such is not directly addressed in international law

- Therefore, there is little legal restraint for state-to-state espionage in general

China is free to impose obligations on its industry, including for the purpose of intelligence collaboration

- But states are in principle also free to ban Chinese products, while respecting their obligations under international trade arrangements

Competition law and public procurement rules may also need to be considered

Such as:

- EU public procurement Directive 2014/24/EU and
- EU electronic communications Directive 2002/21/EC

CCDCOE

Emerging national responses

Emerging national responses vary…

- Strict limitation of Huawei
- Accountability mechanisms
- Accepting risk without further questions

CCDCOE

Conclusions and recommendations

Conclusions

Even though there may be no „smoking gun“, **5G** rollout needs to be recognised as a **strategic rather than merely a technological decision**

Recommendations

- Reaching a **common understanding** of the risks and coordinated approaches among NATO/EU nations
- Setting up **solid risk management mechanisms** (UK)
- Establishing **viable alternatives**, eg strengthening European/Western industry
- Understand that **5G** is an example of a **larger pattern** of Chinese intentional economic and political global expansion

CCDCOE

Thank you!

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

ccdcoe.org
@ccdcoe